

EXHIBIT C

EXHIBIT C

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of NevadaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

265 Lupin Court, Sun Valley, Nevada

Case No. 3:20-mj-071-WGC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
265 Lupin Court, Sun Valley, Nevada as further described in Attachment A, attached hereto and incorporated herein by reference

located in the _____ District of _____ Nevada _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.


The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2251(d)(1)(A), 2252A(a)(1) & (a)(2), 2252A(a) (5)(B), 2252(a)(1) & (a)(2)	Transportation, receipt and distribution, and possession of child pornography

The application is based on these facts:

See attached Affidavit of FBI TFO Gregory Sawyer

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's Signature

FBI TFO Gregory Sawyer

Printed name and title

Subscribed and Sworn to before me by reliable
electronic means.

Date: July 24, 2020



Judge's signature

City and state: Reno, Nevada

WILLIAM G. COBB, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Gregory Sawyer, being first duly sworn, state as follows:

1. I have been employed as a law enforcement officer with the Washoe County Sheriff's Office approximately 22 years and am currently assigned to the Northern Nevada Cyber Center as a Detective. I currently investigate internet-based crimes against children, child sexual exploitation, and other felony crimes involving the use of technology. Further, I am a member of the Federal Bureau of Investigation Child Exploitation Task Force as a sworn TFO and a member of the Nevada Internet Crimes Against Children Task Force. I have received training in excess of 1000 hours in the investigation of internet crimes against children, child sexual exploitation, and computer forensics. I have been actively investigating such cases for the past nine years. The statements contained in this Affidavit are based upon my experience and background as a Special Deputy United States Marshal.

2. I am submitting this Affidavit under Rule 41 of the Federal Rules of Criminal Procedure in support of an Application for a Search Warrant authorizing a search of the residential property at 265 Lupin Court, Sun Valley, Nevada (hereinafter "the Premises"), and this Affidavit is submitted in support of a warrant to search the entire premises, including the residential dwelling, any detached structures, and any computer and computer media located therein where the instrumentalities, fruits and evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, as specified further in Attachment B, might be found. The Premises contain a residence more particularly described in Attachment A.

3. The purpose of this application is to seize evidence, more particularly described in Attachment B, of a violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B),

1 which make it a crime to possess child pornography; and violations of 18 U.S.C. §§
2 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child
3 pornography.

4 4. Because this Affidavit is being submitted for the limited purpose of securing a
5 search warrant, I have not included every fact known to me concerning this investigation. I
6 have set forth only those facts that I believe are necessary to establish probable cause to
7 believe that evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A is located at the
8 Premises, and within computers and related peripherals, and computer media found at 265
9 Lupin Court, Sun Valley, Nevada.

10 5. In summary, the following Affidavit sets forth facts that between April 2019
11 and December 2019, the National Center for Missing and Exploited Children has received
12 nine Cybertips from Google regarding child pornography uploaded to Gmail accounts
13 associated with IP addresses that return to the physical residence located at 265 Lupin Court,
14 Sun Valley, Nevada.

15 6. Administrative subpoenas and Identification checks through the DMV have
16 shown Ryan Eley resides at 265 Lupin Court, Sun Valley, Nevada.

17 7. On July 16, 2020, Detective Adam Harris with the Sparks Police Department
18 downloaded child pornography files from a user on the BitTorrent network in which the IP
19 address returned to the physical residence located at 265 Lupin Court, Sun Valley, Nevada.

20 8. Therefore, I believe there is probable cause to believe someone, most likely a
21 resident of 265 Lupin Court, Sun Valley, Nevada used the internet, specifically Google and
22 the BitTorrent network, to transport, receive, and possess child pornography using a
23 computer or computers that are located at 265 Lupin Court, Sun Valley, Nevada.
24

PERTINENT FEDERAL CRIMINAL STATUTES

9. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors.

10. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

11. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

12. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

13. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B to this Affidavit:

1 a. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8)
2 (any visual depiction of sexually explicit conduct where (a) the production of the visual
3 depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual
4 depiction is a digital image, computer image, or computer-generated image that is, or is
5 indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual
6 depiction has been created, adapted, or modified to appear that an identifiable minor is
7 engaged in sexually explicit conduct.)

8 b. “Child Erotica” means materials or items that are sexually arousing to
9 persons having a sexual interest in minors, but that are not, in and of themselves, obscene or
10 illegal. In contrast to "child pornography," this material does not necessarily depict minors
11 in sexually explicit poses or positions. Some of the more common types of child erotica
12 include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and
13 diaries. See Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Federal
14 courts have recognized the evidentiary value of child erotica and its admissibility in child
15 pornography cases. See *United States v. Vosburgh*, 602 F.3d 519 (3d Cir. 2010) (possession of
16 child erotica is admissible because images suggest that defendant harbors sexual interest in
17 children and to disprove lack of knowledge or mistake); *United States v. Cross*, 928 F.2d 1030,
18 1050 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and
19 collecting non-sexual photographs of children admissible to show intent and explain actions
20 of defendant).

21 c. “Visual depictions” include developed or undeveloped film and
22 videotape, and data stored on computer disk or by electronic means, which is capable of
23 conversion into a visual image. See 18 U.S.C. § 2256(5).

24 d. “Minor” means any person under the age of eighteen years. See 18

1 U.S.C. § 2256(1).

2 e. “Sexually explicit conduct” means actual or simulated (a) sexual
3 intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of
4 the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse;
5 or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. §
6 2256(2).

7 f. “Computer,” as used herein, is defined pursuant to 18 U.S.C. §
8 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data
9 processing device performing logical or storage functions, and includes any data storage
10 facility or communications facility directly related to or operating in conjunction with such
11 device.”

12 g. “Computer hardware,” as used herein, consists of all equipment that
13 can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit
14 electronic, magnetic, or similar computer impulses or data. Computer hardware includes
15 any data-processing devices (including, but not limited to, central processing units, internal
16 and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives
17 and diskettes, and other memory storage devices); peripheral input/output devices
18 (including, but not limited to, keyboards, printers, video display monitors, and related
19 communications devices such as cables and connections), as well as any devices,
20 mechanisms, or parts that can be used to restrict access to computer hardware (including,
21 but not limited to, physical keys and locks).

22 h. “Computer software,” as used herein, is digital information that can be
23 interpreted by a computer and any of its related components to direct the way they work.
24 Computer software is stored in electronic, magnetic, or other digital form. It commonly

1 includes programs to run operating systems, applications, and utilities.

2 i. "Computer-related documentation," as used herein, consists of
3 written, recorded, printed, or electronically stored material that explains or illustrates how
4 to configure or use computer hardware, computer software, or other related items.

5 j. "Internet." As used herein, is a global network of computers and other
6 electronic devices that communicate with each other. Due to the structure of the Internet,
7 connections between devices on the Internet often cross state and international borders, even
8 when the devices communicating with each other are in the same state.

9 k. "Internet Service Providers," or "ISPs," are commercial organizations
10 that provide individuals and businesses access to the Internet. ISPs can offer various means
11 by which to access the Internet including telephone-based dial-up, broadband-based access
12 via a digital subscriber line (DSL) or cable television, or satellite-based subscription. Many
13 ISPs assign each subscriber an account name. By using a computer connected with an
14 internet capable modem, the subscriber can establish a connection to the internet through
15 the ISP service.

16 l. "Internet Protocol address," or "IP address," The Internet Protocol
17 address (or simply "IP address") consists of two versions (IPv4 and IPv6). IP addresses are
18 unique numeric addresses used by digital devices capable of accessing the Internet. An IPv4
19 address looks like a series of four numbers, each in the range 0-255, separated by periods
20 (e.g., 121.56.97.178). There are approximately 4 billion possible addresses using the IPv4
21 standard. IPv6 addresses were developed out of necessity as all the IPv4 addresses have been
22 exhausted due to the explosion of the internet and internet capable devices. IPv6 addresses
23 consist of eight groups of 4 hexadecimal characters. Each group of four hexadecimal
24 characters is separated by a colon. With IPv6 there are forty-two undecillion possible

1 addresses, or approximately 6 octillion addresses for each person on the planet. Every
2 computer attached to the Internet computer must be assigned an IP address so that Internet
3 traffic sent from and directed to that computer may be directed properly from its source to
4 its destination. Most Internet service providers control a range of IP addresses. Some
5 computers have static—that is, long-term—IP addresses, while other computers have
6 dynamic—that is, capable of changing —IP addresses.

7 m. The terms “records,” “documents,” and “materials,” as used herein,
8 include all information recorded in any form, visual or aural, and by any means, whether in
9 handmade form (including, but not limited to, writings, drawings, painting), photographic
10 form (including, but not limited to, microfilm, microfiche, prints, slides, negatives,
11 videotapes, motion pictures, photocopies), mechanical form (including, but not limited to,
12 phonograph records, printing, typing) or electrical, electronic or magnetic form (including,
13 but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage
14 devices such as floppy diskettes, hard drives, CD-ROMs, digital video disks (DVDs),
15 Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical
16 disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic
17 notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical
18 or electronic storage device.

19 n. “Digital device” includes any electronic system or device capable of
20 storing and/or processing data in digital form, including: central processing units; desktop
21 computers; laptop or notebook computers; personal digital assistants; wireless
22 communication devices such as telephone paging devices, beepers, and mobile telephones;
23 peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors,
24 and drives intended for removable media; related communications devices such as modems,

1 cables, and connections; storage media such as hard disk drives, floppy disks, compact disks,
2 magnetic tapes, and memory chips; and security devices.

3 o. "Storage medium or media": A storage medium is any physical object
4 upon which computer data can be recorded. Examples include hard disks, floppy disks, flash
5 memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

6 p. "Imaging" or "copying" refers to an accurate reproduction of
7 information contained on an original physical item, independent of the electronic storage
8 device. "Imaging" or "copying" maintains contents, but attributes may change during the
9 reproduction.

10 q. "Hash value" refers to a mathematical algorithm generated against
11 data to produce a numeric value that is representative of that data. A hash value may be run
12 on media to find the precise data from which the value was generated. Hash values cannot
13 be used to find other data. A hash value can be described as a digital fingerprint for a
14 computer data file. Any alteration of a computer data file would change that file's hash value.

15 **BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS**

16 14. As described above and in Attachment B, this application seeks permission to
17 search for records that might be found on the Premises, in whatever form they are found.
18 One form in which the records might be found is data stored on a computer's hard drive or
19 other storage media. Thus, the warrant applied for would authorize the seizure of electronic
20 storage media or, potentially, the copying of electronically stored information, all under Rule
21 41(e)(2)(B).

22 15. I submit that if a computer or storage medium is found on the Premises, there
23 is probable cause to believe those records will be stored on that computer or storage medium,
24 for at least the following reasons:

1 a. Individuals can transfer images and videos from one electronic device
2 to others through direct connection, scanning, wireless transfer, and other electronic means.

3 b. Computers and other digital storage devices can store large amounts of
4 electronic data, which can include images and videos. This data can be electronically stored
5 virtually anywhere within the file structure on the device. Storage device sizes have
6 continued to increase and the chances of recovering previously deleted content from these
7 devices also has increased as a result of the content being less likely to be overwritten with
8 the increase in storage size.

9 c. As is the case with most digital technology, computer communications
10 can be saved or stored on hardware and computer storage media used for these purposes.
11 Storing of information can occur through intentional acts of saving or downloading files, or
12 by other methods, which automatically occur through normal computer use. This automatic
13 storing of information can be considered “footprints” of use in which the device stores
14 temporary files, links, cached files, opened and accessed files, and history. This information,
15 like any other data can be stored for extensive periods of time until overwritten or
16 intentionally wiped or destroyed. A thorough search of the data contained on these devices
17 could often uncover evidence the crimes listed in this affidavit.

18 d. Data that exists on a computer is particularly resilient to deletion.
19 Computer files or remnants of such files can be recovered months or even years after they
20 have been downloaded onto a hard drive or other storage medium, deleted, or viewed via
21 the Internet. Even when such files have been deleted, they can often be recovered later using
22 readily available forensic tools. When a person “deletes” a file on a home computer, the file
23 is sent to the recycle bin, where it can be easily accessed by the user. Even when a person
24 deletes a file from the recycle bin, the data contained in the file does not actually disappear;

1 rather, that data remains on the hard drive until it is overwritten by new data. Therefore,
2 deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in
3 space on the hard drive that is not allocated to an active file or that is unused after a file has
4 been allocated to a set block of storage space – for long periods of time before they are
5 overwritten. In addition, a computer’s operating system may also keep a record of deleted
6 data in a “swap” or “recovery” file.

7 e. Wholly apart from user-generated files, computer storage media—in
8 particular, computers’ internal hard drives—contain electronic evidence of how a computer
9 has been used, what it has been used for, and who has used it. To give a few examples, this
10 forensic evidence can take the form of operating system configurations, artifacts from
11 operating system or application operation, file system data structures, and virtual memory
12 “swap” or paging files. Computer users typically do not erase or delete this evidence, because
13 special software is typically required for that task. However, it is technically possible to delete
14 this information.

15 f. Similarly, files that have been viewed via the Internet are sometimes
16 automatically downloaded into a temporary Internet directory or “cache.”

17 g. Forensic evidence on a computer or storage medium can also indicate
18 who has used or controlled the computer or storage medium. This “user attribution”
19 evidence is analogous to the search for “indicia of occupancy” while executing a search
20 warrant at a residence. For example, registry information, configuration files, user profiles,
21 e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or
22 absence of malware, and correspondence (and the data associated with the foregoing, such
23 as file creation and last-accessed dates) may be evidence of who used or controlled the
24 computer or storage medium at a relevant time.

1 h. Further, in finding evidence of how a computer was used, the purpose
2 of its use, who used it, and when, sometimes is necessary to establish that a thing is not
3 present on a storage medium. For example, the presence or absence of counter-forensic
4 programs or anti-virus programs (and associated data) may be relevant to establishing the
5 user's intent.

6 16. *Necessity of seizing or copying entire computers or storage media.* In most cases, a
7 thorough search of a premise for information that might be stored on storage media often
8 requires the seizure of the physical storage media and later off-site review consistent with the
9 warrant. In lieu of removing storage media from the premises, it is sometimes possible to
10 make an image copy of storage media. Generally, imaging is the taking of a complete
11 electronic picture of the computer's data, including all hidden sectors and deleted files.
12 Either seizure or imaging is often necessary to ensure the accuracy and completeness of data
13 recorded on the storage media, and to prevent the loss of the data either from accidental or
14 intentional destruction. This is true because of the following:

15 a. The time required for an examination. As noted above, not all evidence
16 takes the form of documents and files that can be easily viewed on site. Analyzing evidence
17 of how a computer has been used, what it has been used for, and who has used it requires
18 considerable time, and taking that much time on premises could be unreasonable. As
19 explained above, because the warrant calls for forensic electronic evidence, it is exceedingly
20 likely that it will be necessary to examine storage media thoroughly to obtain evidence.
21 Storage media can store a large volume of information. Reviewing that information for
22 things described in the warrant can take weeks or months, depending on the volume of data
23 stored, and would be impractical and invasive to attempt on-site.

24 b. Technical requirements. Computers can be configured in several

1 different ways, featuring a variety of different operating systems, application software, and
2 configurations. Therefore, searching them sometimes requires tools or knowledge that might
3 not be present on the search site. The vast array of computer hardware and software available
4 makes it difficult to know before a search what tools or knowledge will be required to analyze
5 the system and its data on the Premises. However, taking the storage media off-site and
6 reviewing it in a controlled environment will allow its examination with the proper tools and
7 knowledge.

8 c. Variety of forms of electronic media. Records sought under this
9 warrant could be stored in a variety of storage media formats that may require off-site
10 reviewing with specialized forensic tools and software.

11 17. *Nature of examination.* Based on the foregoing, and consistent with Rule
12 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to
13 review the media on-site, the warrant I am applying for would permit seizing or imaging
14 storage media that reasonably appear to contain some or all of the evidence described in the
15 warrant, thus permitting its later examination consistent with the warrant. The examination
16 may require techniques, including but not limited to computer-assisted scans of the entire
17 medium, that might expose many parts of a hard drive to human inspection in order to
18 determine whether it is evidence described by the warrant.

19 18. Because it may be determined other computer users could share the Premises
20 as a residence, it is possible that the Premises will contain computers that are predominantly
21 used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless
22 determined that that it is possible that the things described in this warrant could be found on
23 any of those computers or storage media, the warrant applied for would permit the seizure
24 and review of those items as well. Efforts would normally be taken during the search to

1 minimize seizing of unrelated evidence through onsite computer forensic previewing when
2 possible.

3 a. Similarly, files that have been viewed via the Internet are sometimes
4 automatically downloaded into a temporary Internet directory or "cache."

5 **BACKGROUND ON CHILD EXPLOITATION WITH THE USE OF**
6 **TECHNOLOGY AND OFFENDER CHARACTERISTICS INVOLVING SUCH**
7 **ACTS**

8 19. Based upon my knowledge, training, and experience in online child
9 exploitation and child pornography investigations, and the experience and training of other
10 law enforcement officers with whom I have had discussions, computers and computer
11 technology have revolutionized the way in which child pornography is produced, distributed,
12 stored and communicated as a commodity and a further tool of online child exploitation.

13 20. Based upon my knowledge, experience, and training in child pornography
14 investigations, and the training and experience of other law enforcement officers with whom
15 I have had discussions, I know there are certain characteristics common to individuals
16 involved in the transportation, distribution receipt and possession of child pornography.
17 Those who transport, distribute, receive and/or possess child pornography. These
18 individuals:

19 a. May receive sexual gratification, stimulation, and satisfaction from
20 contact with children; or from fantasies they may have viewing children engaged in sexual
21 activity or in sexually suggestive poses, such as in person, in photographs, or other visual
22 media; or from literature describing such activity.

23 b. May collect sexually explicit or suggestive materials, in a variety of
24 media, including photographs, magazines, motion pictures, videotapes, books, slides and/or

1 drawings or other visual media. Such individuals often use these materials for their own
2 sexual arousal and gratification. Further, they may use these materials to lower the
3 inhibitions of children they are attempting to seduce, to arouse the selected child partner, or
4 to demonstrate the desired sexual acts.

5 c. Often possess and maintain “hard copies” of child pornographic
6 material, which is, their pictures, films, video tapes, magazines, negatives, photographs,
7 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their
8 home or some other secure location. These individuals typically retain pictures, films,
9 photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists,
10 child erotica, and videotapes for many years. These individuals may be referred to as
11 “collectors.”

12 d. Often maintain their collections that are in a digital or electronic format
13 in a safe, secure and private environment, such as a computer and surrounding area. These
14 collections are often maintained for several years and may be kept close by, usually at the
15 individual’s residence, to enable the collector to view the collection, which is valued highly.
16 The collections are often backed up on external devices or other digital media. These
17 “collectors” claim to be unable to delete or be without the material for any extended period.
18 These “collectors” may also choose to store their material online using “cloud” based file
19 storage provided by Internet Service Providers (ISP). This “cloud” based storage allows an
20 offender to store the material on servers maintained by ISPs and access the material
21 anywhere in the world through an internet connection.

22 e. May correspond with and/or meet others to share information and
23 materials; often maintain correspondence from other child pornography
24 distributors/collectors; may conceal such correspondence as they do their sexually explicit

1 material; and often maintain lists of names, addresses, and telephone numbers of individuals
2 with whom they have been in contact and who share the same interests in child pornography.

3 f. May engage in a pattern of continual activity involving the download
4 and sharing of child pornography for sexual gratification, regardless of their actions of
5 storing, collecting, or deleting the material.

6 g. May take steps to avoid detection by intentionally downloading,
7 viewing, and maintaining dominion and control of child pornography related material to
8 achieve sexual gratification, then purposely deleting the material until choosing to download
9 again. Individuals previously showing traits as a “collector” may have transitioned into a
10 deleting behavior pattern due to the ease and accessibility of child pornography through the
11 internet.

12 h. May collect non-sexually explicit images and/or videos of children
13 relating to their preference concerning age, sex, hair color, body type, and other physical
14 characteristics and maintain those images in similar manner as the child pornography
15 described above.

16 i. May organize, catalog, and separate their collections based on physical
17 characteristics of the children, series, or scene types and settings.

18 j. Often download large quantities of child pornography during online
19 sessions and later filter through the material to locate the desirable content to save based
20 upon the offender’s preferences at the time or to determine if the file is already in their
21 possession.

22 k. Sometimes enjoy and maintain both adult and child pornography
23 ranging in broad types of scene content or portrayal from voyeuristic nudity to brutal rape
24 scenes. Offender’s preferences of the scene settings often change from time to time in addition

1 to showing a progression towards more sexually explicit material.

2 **INFORMATION REGARDING GOOGLE**

3 21. Google provides multiple services for users including email and cloud storage.
4 Subscribers obtain an account by registering with Google. Once a Google account is created,
5 the user is provided 15 GB (gigabytes) of free online "cloud" based storage, accessible
6 through their gmail.com account or through accessing the Google.com website. The users'
7 devices can also be backed up to this account. Additional storage space is available for a fee.

8 22. Google provides an IP log for the account in question when submitting a
9 Cybertip to NCMEC. Multiple IP addresses are often included in this IP log as users are
10 very often utilizing mobile devices (smartphones) to access their Google accounts. In order
11 to maintain functionality a smartphone will switch between sources of internet service (such
12 as residential internet service or internet service provided by their cell phone service carrier).
13 As such there are instances when the uploaded file may not have originated from the user's
14 residence, but instead from the internet source wherever the phone may be at the time of the
15 upload. However, almost always the IP address of the user's residence is repeatedly listed in
16 the IP logs. This is a result of the user travelling to and from their home combined with a
17 feature frequently programmed into smartphones to prefer a connection to WIFI over a
18 connection to cellular data. This is commonly done as most cell phone plans require the
19 subscriber to pay for data where residential internet most often has a fixed cost.

20 23. In my training and experience, I have learned that many Android cellular
21 phones (Android is owned by Google) backup users' photos and videos to their Google cloud
22 storage account by default, leading to the generation of Cybertips in cases involving child
23 pornography. Additionally, when a Google account is added to an iPhone a users' photos
24 and video can be uploaded to Google's cloud storage.

DETAILS OF THE INVESTIGATION

24. Pursuant to 18 U.S.C. § 2258A, Electronic Service Providers are required to report incidents of child pornography to the National Center for Missing and Exploited Children (NCMEC) through the “CyberTipline.”

25. The National Center for Missing and Exploited Children compiles the information from the ESP then forwards the reported information to law enforcement operating in the area where the activity is believed to be occurring or originated from. This report is called a “CyberTip.”

26. On April 12, 2019, The National Center for Missing and Exploited Children (NCMEC) received information submitted electronically to the CyberTipline by Electronic Service Provider (ESP) Google, Inc. regarding Child Pornography (possession, manufacture, and distribution) and assigned it CyberTipline Report number 485458864.

27. On May 14, 2019, The National Center for Missing and Exploited Children (NCMEC) received information submitted electronically to the CyberTipline by Electronic Service Provider (ESP) Google, Inc. regarding Child Pornography (possession, manufacture, and distribution) and assigned it CyberTipline Report number 49594473.

28. On December 5, 2019, The National Center for Missing and Exploited Children (NCMEC) received information submitted electronically to the CyberTipline by Electronic Service Provider (ESP) Google, Inc. regarding Child Pornography (possession, manufacture, and distribution) and assigned it CyberTipline Report number 60635340.

29. CyberTipline Report number 48545864 contained information received from Google, Inc. regarding files containing suspected child pornography that were uploaded and stored in Google Photos infrastructure by a subject using email address of gangbangin6669@gmail.com. Google provided a backup email address for the account

1 listed above. The backup email account is ryaneley@yahoo.com. I viewed the files and
2 based on my training and experience; I believe one of the files contain child pornography.
3 The picture from CyberTipline 48545864, Filename: 4903df20-8cea-4d17-ae49-
4 fea6f67d2385.jpg, depicts a young girl approximately eight to twelve years of age. The girl
5 is lying on her back with her face not showing. The girl is lying on a pink blanket and is
6 wearing a blue skirt with white stripes and no underwear. The skirt is pulled up to the girls'
7 stomach area exposing her vagina.¹ Google, Inc. identified login IP information for this
8 account within the CyberTipline Reports. The IP address at the time the image was uploaded
9 was 2600:6c4e:a00:5e46:dcde:3b77:4bcf:45de (IPv6 address). A check of that IPv6 address
10 found it to belong to Charter Communications. It should be noted that IPv6 is a new version
11 of IP addressing that was developed as a result of the IPv4 address supply has been
12 exhausted. Charter Communications currently utilizes a "dual stack" approach which
13 means they utilize both IPv4 (traditional IP addresses) and IPv6 simultaneously. Providers
14 such as Google can capture either a IPv6 address or an IPv4 address.

15 30. An Agent with HSI sent an administrative subpoena to Charter
16 Communications to provide information pertaining to the IP addresses listed above.

17 31. On May 30, 2019, Charter Communications responded stating that the above
18 IP addresses resolved back to accountholder Ryan Ely 265 Lupin Court, Sun Valley, NV,
19 89433. Charter provided email addresses associated with the account. Examples of those
20 are: ryanely666@charter.net and ryanely18@yahoo.com. Charter Communications has the
21 subscriber's last name spelled as Ely. A check of the subject's last name in the DMV database
22

23 ¹ Undersigned will present each image and representative images from each
24 individual video depicting child pornography described in this affidavit and make those
images available for review by the Magistrate Judge in determining probable cause.

1 and the Washoe County Sheriff's Office database shows the correct spelling is Eley.

2 32. CyberTipline Report number 60635340 contained information received from
3 Google, Inc. regarding files containing suspected child pornography that were uploaded and
4 stored with Google by a subject using an email address of
5 hotandreadywhenyouare123@gmail.com. Google provided an IP address from which the
6 account had been accessed. The IP address is 71.89.252.164. One of the files uploaded to
7 Google from hotandreadywhenyouare123@gmail.com, which I viewed, can be described as
8 a two-minute video of a 6 – 8-year-old girl who is nude from the waist down and wearing a
9 blue Dr. Seuss Cat in the Hat t-shirt. The young girl is being anally or vaginally penetrated
10 by an adult male penis. The file name is: Google-CT-RPT-
11 a2a023de0c5c9685fe67a4902c50b4d7-VID-20170223-WA0052.mp4.

12 33. On February 13, 2020 a Detective with the Sparks Police Department sent an
13 Administrative Subpoena to Charter Communication requesting subscriber information
14 associated with the IP address 71.89.252.164.

15 34. On March 5, 2020, Charter Communications responded stating that the above
16 IP addresses resolved back to accountholder Ryan Ely 265 Lupin Court, Sun Valley, NV,
17 89433. Charter provided email addresses and a phone number associated with the account.
18 The email addresses are: ryanely666@charter.net and theresaip76@charter.net. The phone
19 number is 775-737-4182. A check of the Washoe County Sheriff's Office database showed
20 Ryan Eley listed this phone number as his cell phone number in September 2019.

21 35. Based on the subpoena information, I believe the suspect used the Google
22 accounts gangbangin6669@gmail.com, ryanel420@gmail.com, and
23 hotandreadywhenyouare123@gmail.com to upload child pornography files. The suspect
24 accessed the internet using IP addresses returning to 265 Lupin Court, Sun Valley, Nevada.

1 36. On July 16, 2020, Detective Harris downloaded multiple child pornography
2 files via the BitTorrent network from the IP address 71.89.252.164. This is the same IP
3 address associated with the Google Cybertips that resolved to the physical address 265 Lupin
4 Court, Sun Valley, Nevada. Examples of the child pornography downloaded are as follows:

5 A. File Name: 23.08.2005 0-39-32_0074.jpg

6 Description: This is an image of a 6 to 10 year old female child in a
7 wooded area. The child is fully nude with a pair of underwear around her
8 knees. The child's vagina is fully exposed.

9 B. File Name: 23.08.2005 0-40-26_0084.jpg

10 Description: This is an image of a 6 to 10 year old female child in a
11 wooded area. The child is kneeling on a tree branch, is fully nude with
12 her legs spread, and is urinating.

13 C. File Name: 23.08.2005 0-41-25_0095.jpg

14 Description: This is an image of a 6 to 8 year old female child. The child
15 is fully nude lying on a kids blanket. The child is separating her labia and
16 exposing her vagina.

17 37. Based on my training and experience, I know that Charter issues a dynamic
18 IP address to its residential customers. A dynamic IP address may change where a static IP
19 address is fixed. However, I know that the IP addresses assigned by Charter to their
20 customers very rarely change.

21 38. On July 16, 2020 Detective Harris sent an Administrative Subpoena to Charter
22 requesting the subscriber information for the IP address 71.89.252.164 on July 16, 2020.

23 39. On July 17, 2020 Charter responded to the Administrative Subpoena and
24 identified 265 Lupin Court, Sun Valley, Nevada as the physical address associated with IP

1 address 71.89.252.164 and Ryan Ely as the subscriber.

2 40. A check of the Nevada Department of Motor Vehicles shows Ryan Eley listed
3 265 Lupin Court, Sun Valley, Nevada as his address on his Nevada Identification Card.

4 41. I know that a computer may be utilized by more than one person at a single
5 residence and the possibility of unsecured wireless and/or computer intrusion may exist until
6 excluded. Therefore, I have identified the possible suspects in this case as Ryan Eley, and/or
7 John / Jane Doe. In the unlikely event of unsecured wireless being accessed by another
8 individual not residing within the residence, the crimes and communication would still be
9 occurring through the computer, modem, or router located at this residence as identified by
10 the ISP. This activity would likely be identified during the service of the search warrant
11 during an onsite digital evidence preview. The modem or router at the service address
12 identified within this warrant processes the communications. Routers are also capable of
13 storing log information, which could identify any other computers connected to it.

14 **RETURN AND REVIEW PROCEDURES**

15 Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

16 (f) Executing and Returning the Warrant.

17 (1) Warrant to Search for and Seize a Person or Property.

18 (2) Inventory. An officer present during the execution of the warrant
19 must prepare and verify an inventory of any property seized.

20 42. (D) *Return*. The officer executing the warrant must promptly return it—
21 together with a copy of the inventory—to the magistrate judge designated on the warrant.
22 The officer may do so by reliable electronic means. The judge must, on request, give a copy
23 of the inventory to the person from whom, or from whose premises, the property was taken
24 and to the applicant for the warrant.

1 43. Pursuant to this Rule, I understand and will act in accordance with the
2 following:

3 a. Rule 41(f)(1)(D) requires that an agent file with the court an inventory
4 return, an itemized list of the property seized, in a prompt manner.

5 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
6 which electronically stored information must be seized after the issuance of the warrant or
7 copied after the execution of the warrant, not the “later review of the media” that was seized.
8 The requirement for the timing and filing of the return is not the same as the requirement for
9 the forensic review of the seized items.

10 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the
11 court may be limited to a description of the “physical storage media or information” seized or
12 copied, not an itemization of the information or data stored on the “physical storage media.”

13 d. Written permission is necessary to retain copies of seized items and data
14 after the completion of the forensic review. I request that authorization herein, and will renew
15 by request as the court deems necessary, to retain copies, as many as are necessary to create
16 pursuant to other requirements set forth in or imposed by the court, of the seized media after
17 the completion of the forensic review through the investigation and final disposition of any
18 charges filed against the person subject to this warrant based upon the seized media. This
19 judicial authorization is appropriate in this matter because.

20 i. Should the execution of the warrant uncover data that may later
21 need to be introduced into evidence during a trial or other proceeding, the authenticity and the
22 integrity of the evidence and the government’s forensic methodology may be contested issues.
23 Retaining copies of seized storage media can be required to prove these facts.
24

1 ii. Returning the original storage medium to its owner will not allow
2 for the preservation of that evidence. Even routine use may forever change the data it contains,
3 alter system access times, or eliminate data stored on it. Additionally, I have probable cause to
4 believe that the original storage media in this case will be found to contain contraband. Law
5 enforcement officers cannot legally return contraband to citizens.

6 iii. Because the investigation is not yet complete, it is not possible to
7 predict all possible defendants against whom evidence found on the storage medium might be
8 used. That evidence might be used against persons who have no possessory interest in the
9 storage media, or against persons yet unknown. Those defendants might be entitled to a
10 copy of the complete storage media in discovery. Retention of a complete image assures that
11 it will be available to all parties, including those known now and those later identified.


12 iv. The act of destroying or returning original storage media could
13 create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage
14 medium contained evidence favorable to him. Maintaining a copy of the storage medium
15 would permit the government, through an additional warrant if necessary, to investigate such
16 a claim.

17 v. Similarly, should a defendant suggest an explanation for the
18 presence of evidence on storage media, it may be necessary to investigate such an explanation
19 by, among other things, re-examining the storage medium with that defense in mind. This
20 may require an additional examination of the storage medium for evidence that is described
21 in Attachment B but was not properly identified previously.

22 vi. In its search warrant return to be filed with this Court, the
23 government will certify that it has retained identified items as instrumentalities of the crime
24 being investigated, as well as at least one mirror image of each device.


CONCLUSION

44. Based on the foregoing, there is probable cause to believe that Title 18 U.S.C. §§ 2251, 2252 and 2252A, which, among other things, makes it a federal crime for any person to transport, possess, receive or distribute child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at 265 Lupin Court, Sun Valley, Nevada as more fully described in Attachment A.



Gregory Sawyer
FBI Task Force Officer

Subscribed and Sworn before me by reliable electronic means before me this 24th day of July, 2020.



HON. WILLIAM G. COBB
United States Magistrate Judge

ATTACHMENT A
PREMISES TO BE SEARCHED

265 Lupin Court, Sun Valley, Nevada

The residence to be searched is located at 265 Lupin Court, Sun Valley, Nevada. The residence is described as a brown single-story mobile home. The number 265 is affixed to the front right corner of the home when looking from the street.



ATTACHMENT B**LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED**

This Affidavit is in support of application for a warrant to search the premises known as 265 Lupin Court, Sun Valley, Nevada which is more specifically identified in the body of the application and in Attachment A, including any computers, associated storage devices and/or other devices located therein that can be used to store information and/or connect to the Internet, for records and materials evidencing a violation of 18 U.S.C. §§ 2252(a)(1) and 2252A(a)(1), which make it a crime to transport or ship in interstate or foreign commerce, by computer, child pornography; 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography; and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography (defined in 18 U.S.C. § 2256), as more specifically identified below:

1. Any and all computers, computer system and related peripherals, cellular telephones, personal digital assistants, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, storage media (including but limited to items specifically listed elsewhere in this paragraph, and further including but not limited to magnetic media floppy disks, tape systems, compact discs, digital video discs, Blu-Ray discs, thumb drives and hard drives), terminals (keyboards and display screens) and other computer related operation equipment, in addition to computer photographs, digital graphic file formats and/or photographs, slides or other visual depictions of such digital graphic file format equipment that may be, or are used to visually depict child pornography, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession, or receipt of child pornography, or information

1 pertaining to an interest in child pornography.

2 2. Any and all material depicting child pornography, any sexual conduct
3 regardless of whether it is between adult(s) and children, or between children, child erotica; any
4 images, visual recording, digital imagery, sketches, drawings, or other media depicting or
5 portraying lewd or lascivious exhibition of children's genitalia; sexually suggestive poses
6 involving children; or any type of sexually explicit conduct involving children, as defined in
7 Title 18, United States Code, Section 2256(8). Any and all audio recordings involving children
8 engaging in sexual acts, whether alone, with another child or children, or with an adult or
9 adults.

10 3. Any and all computer software, including programs to run operating
11 systems, applications (like word processing, graphics, or spreadsheet programs), utilities,
12 compilers, interpreters, and communications programs.

13 4. Any computer-related documentation, which consists of written,
14 recorded, printed or electronically stored material that explains or illustrates how to configure
15 or use computer hardware, software or other related items.

16 5. Any and all records and materials, in any format and media (including,
17 but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages),
18 pertaining to the possession, receipt or distribution of visual depictions of minors engaged in
19 sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

20 6. In any format and media, all originals, copies and negatives of visual
21 depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States
22 Code, Section 2256.

23 7. Any and all cameras, camera equipment, photography equipment or any
24 other digital device capable of recording or storing sexually explicit images of minors in

1 negative, digital or other format.

2 8. Any and all records and materials, in any format and media (including,
3 but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages)
4 identifying persons transmitting through interstate or foreign commerce, including via
5 computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in
6 Title 18, United States Code, Section 2256.

7 9. Any and all records and materials, in any format and media (including,
8 but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital
9 data files and web cache information), bearing on the receipt, shipment or possession of visual
10 depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States
11 Code, Section 2256.

12 10. Records of communication (as might be found, for example, in digital
13 data files) between individuals concerning the topic of child pornography, the existence of sites
14 on the Internet that contain child pornography or who cater to those with an interest in child
15 pornography, as well as evidence of membership, subscription or free membership, in online
16 clubs, groups, services, or other Internet sites that provide or make accessible child pornography
17 to its members and constituents.

18 11. Evidence of any online storage, e-mail or other remote computer storage
19 subscription to include unique software of such subscription, user logs or archived data that
20 show connection to such service, and user login and passwords for such service.

21 12. Records evidencing occupancy or ownership of the premises described
22 above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed
23 correspondence.

24 13. Records, in any format or media, evidencing ownership or use of

1 computer equipment and paraphernalia found in the residence to be searched, including, but
2 not limited to, sales receipts, registration records, records of payment for Internet access, records
3 of payment for access to newsgroups or other online subscription services, handwritten notes
4 and handwritten notes in computer manuals.

5 14. Any and all buddy lists, correspondence, or text messages in whatever
6 media and format pertaining to Group E-Mails which relate to child exploitation or child
7 pornography.

8 15. Images and videos of children in non-sexually explicit poses or scenes,
9 located in electronic, digital, or printed formats, which are necessary for comparison purposes
10 of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18,
11 United States Code, Section 2256.

12 16. Any and all records, in any format, relating to or showing use of peer-to-
13 peer filing sharing programs and software.

14 17. For any computer, computer hard drive, or other physical object upon
15 which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this
16 warrant, or that might contain things otherwise called for by this warrant:

17 a. Evidence of who used, owned, or controlled the COMPUTER at
18 the time the things described in this warrant were created, edited, or deleted, such as logs,
19 registry entries, configuration files, saved usernames and passwords, documents, browsing
20 history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and
21 correspondence;

22 b. Evidence of software that would allow others to control the
23 COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as
24 evidence of the presence or absence of security software designed to detect malicious software;

- 1 c. Evidence of the lack of such malicious software;
- 2 d. Evidence of the attachment to the COMPUTER of other storage
- 3 devices or similar containers for electronic evidence;
- 4 e. Evidence of counter-forensic programs (and associated data) that
- 5 are designed to eliminate data from the COMPUTER;
- 6 f. Evidence of the times the COMPUTER was used;
- 7 g. Passwords, encryption keys, and other access devices that may be
- 8 necessary to access the COMPUTER.